Available online at www.sciencedirect.com
SciVerse ScienceDirect
Electronic Notes in Theoretical Computer Science
Electronic Notes in Theoretical Computer Science 276 (2011) 145–158
www.elsevier.com/locate/entcs

A Quantum Representation for Involution Groups

Tanner Crowder[1,2]

Naval Research Laboratory
Center for High Assurance Computer Systems
Washington DC 20375

Abstract

We answer a question posed by Martin et al. at MFPS XXVI in the affirmative: the free affine monoid over a finite involution group has a quantum representation, in addition to the classical representation already shown to exist in [8]. In particular, this implies that in every dimension there are non-trivial classes of quantum channels that have classical representations which were not present in the lower dimensions. En route to establishing this result, we give two characterizations of the diagonal n-qubit channels (one of which is stated in [1]) and necessary conditions for a Bloch matrix to satisfy.

Keywords: Bloch representation, free object, quantum channel, involution group.

1 Introduction

A classical channel with m inputs and n outputs can be represented by a $m \times n$ stochastic matrix; the set of these channels is denoted (m, n). One way to transmit information through a qubit channel is to fix a basis in the state space, $\{|\psi\rangle, |\phi\rangle\}$, and let $|\psi\rangle$ and $|\phi\rangle$ represent 0 and 1, respectively. Using this basis we can define a $(2, 2)$ classical channel which has capacity

$$C(x, y) = \log_2 \left(2^{\frac{\bar{x}H(y) - \bar{y}H(x)}{x-y}} + 2^{\frac{yH(x) - xH(y)}{x-y}} \right),$$

where $x = P(0|0), y = P(0, 1)$ and $H(x) = -x \log_2(x) - (1 - x) \log_2(1 - x)$. The capacity measures the amount of classical information that can be transmitted through the qubit channel. For a qubit channel, each choice of a basis defines a classical channel, each with its own capacity. The scope of a qubit channel is the

[1] The author is a graduate student in the mathematics department at Howard University
[2] Email: tanner.crowder@nrl.navy.mil

1571-0661 Published by Elsevier B.V.
doi:10.1016/j.entcs.2011.09.019

range of capacities obtained when varying over all bases in the state space. Calculating $C(x, y)$ for an arbitrary basis is a tedious task, and thinking about calculating capacity for every basis in the state space makes us shudder.

In [11], Martin reduced the calculation of scope to a simple eigenvalue calculation. Moreover, there are classes of (m, n) channels which carry information theoretic data about certain classes of unital qubit channels. The classes are well studied and were shown to be conjugate to their quantum counterparts [4,5,9]; since conjugation preserves eigenvalues, the scope and capacity of these channels can be calculated from the classical representations.

The natural question arises whether there is a higher dimensional analog to calculating scope and are there classes of (m, n) classical channels that carry similar information theoretic data about multi-qubit channels. Attempting to extend the results from the qubit case requires more information about the Bloch representation of the higher dimensional quantum channels. In the case of a qubit, the set of Bloch matrices is the convex closure of SO(3). However, for $n \geq 2$ it is only known that the set of n-qubit Bloch matrices is a proper subset of the convex closure of $\mathrm{SO}(2^{2n}-1)$. Here we will give two characterizations of the diagonal Bloch matrices of arbitrary dimension. The first gives 2^{2n} inequalities for the elements of a diagonal matrix to satisfy; these are necessary and sufficient conditions stated in [1] which we will prove in full generality. We will then show those conditions are equivalent to taking the convex closure of a finite set of 2^{2n}-many diagonal matrices. More importantly, for the involution groups of order 2^{2n} and 2^{2n-1}, there is an isomorphism defined by conjugation from the classical representations of their free affine monoids into the set of unital n-qubit channels via the Bloch representation. Lastly, we will extend the trace condition, found in [11], to an arbitrary n-qubit channel and give a lower bound for the scope of a channel.

2 Preliminaries

In order to discuss quantum channels we need a way to talk about how an environment acts on quantum systems and a way of describing a system whose state is not completely known. We use density operators/matrices (the terms are used interchangeably) to describe a quantum system. Let $\mathcal{H}^{2^n}$ be a Hilbert space of dimension 2^n.

Definition 2.1 A quantum state is a self adjoint, positive semi-definite, trace one, linear operator $\rho : \mathcal{H}^{2^n} \to \mathcal{H}^{2^n}$ which is called a *density operator*; when the operator is represented by a matrix it is called a *density matrix*. The set of density matrices on n-qubits is denoted Ω^{2^n}.

If a quantum system can be in states $|\psi_i\rangle \in \mathcal{H}^{2^n}$ with probabilities p_i, then the density matrix can be written as $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$, where we take each $|\psi_i\rangle$ to be normalized. It is clear that ρ is a density matrix for an n-qubit system if and only if it is a $2^n \times 2^n$ trace one, positive semi-definite, Hermitian matrix. The $2^n \times 2^n$ Hermitian matrices form a vector space over $\mathbb{R}$ of dimension 2^{2n}, so there are $2^{2n}-1$

Hermitian matrices, $\lambda = \{\lambda_i\}_{i=2}^{2^{2n}}$, such that $\{I_{2^n}\} \cup \lambda$ is a basis. It is well known that for the real vector space of 2×2 Hermitian matrices, the identity along with the spin operators, or Pauli Matrices, are a basis:

$$\sigma_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_4 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Definition 2.2 Define $\left\{ \frac{1}{\sqrt{2^{n-1}}} \sigma_{j_1} \otimes \cdots \otimes \sigma_{j_n} | j_i \in \{1,2,3,4\} \right\}$ to be the set of *n-qubit spin operators*; we will order them with the dictionary order.

We call the i^{th} matrix in this order λ_i^n (n denotes the dimension of the system and will be dropped when confusion does not arise). Typically we will represent the last $2^{2n} - 1$ elements in vector form as $\lambda = [\lambda_2\ \lambda_3 \cdots \lambda_{2^{2n}}]$. Given two vector spaces V and W with their respective bases, $\{|v_i\rangle\}$ and $\{|w_j\rangle\}$, $\{|v_i\rangle \otimes |w_j\rangle\}$ is a basis for $V \otimes W$ (see [13] for properties of the tensor product). It is immediate that the n-dimensional spin operators form a linearly independent set contained in the $2^n \times 2^n$ Hermitian matrices, and since there are 2^{2n} of them, they must form a basis. Thus, every density matrix can be written as some linear combination of n-dimensional spin operators (with certain constraints), i.e., every density matrix for an n-qubit system can be written as

$$\rho = \frac{I + cr \cdot \lambda}{2^n},$$

where $c = \sqrt{\frac{2^{2n} - 2^n}{2}}$ and λ is the vector of the n-dimensional spin operators (without the identity).

Definition 2.3 The vector r in the above expansion of a density matrix is called the *Bloch vector*.

It is well known that for this decomposition to describe a quantum state, $r \in \mathbb{B}^{2^{2n}-1}$ (the unit ball of dimension $2^{2n} - 1$), but for $n \geq 2$ the Bloch vectors form a proper subset of $\mathbb{B}^{2^{2n}-1}$ [6]. Note that sometimes we will absorb c into the Bloch vector. A density operator ρ describes a pure state if its state $|\psi\rangle$ is completely known, i.e., $\rho = |\psi\rangle\langle\psi|$, otherwise it is a mixed state; the constant c ensures that the Bloch vector of a pure state has norm 1.

A quantum channel is a medium used to send quantum states. These channels can be modeled by maps on the set of density matrices that fulfill certain natural intuitions. Consider a quantum channel $\epsilon : \Omega^{2^n} \to \Omega^{2^n}$. If we were selecting a quantum state from a distribution $\{|\psi_i\rangle\}$ with probability p_i and then applying ϵ, we would expect the output to be the same as if were selecting a quantum state from $\{|\epsilon(\psi_i)\rangle\}$ with probability p_i. Thus we would expect ϵ to be convex-linear. Since ϵ takes density matrices to density matrices it should be a positive map, i.e., it takes positive semi-definite operators to positive positive semi-definite operators. Similarly it must take trace one operators to trace one operators, and thus must

be trace preserving. Moreover, $(\forall m \in \mathbb{N}^+)\ I_m \otimes \epsilon$ should be positive; this property is called *complete positivity*. Complete positivity ensures that if ϵ acts on just one part of a joint system, $I_m \otimes \epsilon$ is still a quantum channel.

Definition 2.4 A *quantum channel* $\Phi : \Omega^{2^n} \to \Omega^{2^n}$ is a completely positive, trace preserving, convex-linear map. It is *unital* provided that the identity is a fixed point.

By Choi's theorem [2], a linear operator on the complex $N \times N$ matrices, $\Phi : M_N \to M_N$, is completely positive if and only if it has the form

$$\Phi(\rho) = \sum_i E_i \rho E_i^\dagger,$$

where the E_i are complex matrices. We have the following characterization, called the *operator sum representation*, of quantum channels found in [12]: The map $\Phi : \Omega^{2^n} \to \Omega^{2^n}$ is a completely positive, trace preserving, convex-linear map if and only if it has the form

$$\Phi(\rho) = \sum_{i=1} A_i \rho A_i^\dagger$$

where $\{A_i\}$ is a collection of operators on Ω^{2^n} and $\sum_i A_i^\dagger A_i = I$. A map of this form clearly preserves hermiticity, so given Choi's theorem and the operator sum representation of a quantum channel, every quantum channel is the restriction of a completely positive, linear map on the Hermitian matrices. Since we have formulated our density matrices in terms of Hermitian matrices, we will view a map on Ω^{2^n} as a map on the $2^n \times 2^n$ Hermitian matrices, H_{2^n}. Since a quantum channel maps a density matrix to a density matrix, it must induce a map ϕ on the Bloch vector:

$$\Phi\left(\frac{I + cr \cdot \lambda}{2^n}\right) = \frac{I + c\phi(r) \cdot \lambda}{2^n}.$$

These maps are of critical importance in understanding the scope and capacity of a qubit channel, and we will devote most of this note to investigating them.

Lemma 2.5 *Every quantum channel induces an affine map on the Bloch vector. When the channel is unital, the affine map is linear.*

Proof. Let $N = 2^n$ and $\Phi : H_N \to H_N$ be a linear map with the property $\Phi(I + r \cdot \lambda) = I + s \cdot \lambda$. Consider an arbitrary element of H_N, $\rho_1 = \sum_i x_i \lambda_i$, and take $\rho_2 = \sum_i y_i \lambda_i = \Phi(\rho_1)$. Let $M = (a_{ij})$ be the matrix of the operator Φ, then

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_N \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1N} \\ a_{21} & a_{22} & \cdots & a_{2N} \\ \vdots & & & \vdots \\ a_{N1} & a_{N2} & \cdots & a_{NN} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_N \end{pmatrix}.$$

By assumption, if $x_1 = 1$ then $y_1 = 1$. Also, if $x_1 = 1$ then for $i \geq 2$, $y_i = \sum_{j=2}^N a_{ij} x_j + a_{i1}$. Let $b = [a_{21}\ a_{31} \cdots a_{N1}]^t$, $y = [y_2\ y_3 \cdots y_N]^t$, and

$x = [x_2\ x_3 \cdots x_N]^t$. Then $y = \tilde{M}x + b$, where

$$\tilde{M} = \begin{pmatrix} a_{22} & \cdots & a_{2N} \\ \vdots & \ddots & \vdots \\ a_{N2} & \cdots & a_{NN} \end{pmatrix}.$$

Therefore, if ρ_1 is a density matrix, $\Phi(\rho_1) = 1/2^n(I + (\tilde{M}x + b) \cdot \lambda)$. To compute $\Phi(I)$, we take x to be the zero vector; for $\Phi(I) = I$ it is immediate that b must also be the zero vector. □

Definition 2.6 Let $\rho = 1/2^n(I + cr \cdot \lambda)$ be a density matrix and let Φ be a quantum channel defined as

$$\Phi(\rho) = \frac{I + c(Ar + b) \cdot \lambda}{2^n}.$$

This is the *Bloch representation* of the channel Φ and A is the *Bloch matrix* associated with Φ. We will sometimes refer to Φ as Φ_{Ax+b} to put emphasis on the Bloch representation.

Define the set of Bloch representations on n-qubits to be $\mathcal{Q}_n$ and the unital Bloch representations to be $\mathcal{U}_n$. There are multiple operator sum representations for one quantum channel; for example if U_i and V_i differed by a phase then for each $\rho \in \Omega^{2^n}$, $\sum_i U_i \rho U_i^\dagger = \sum_i V_i \rho V_i^\dagger$. So for Definition 2.6 to make sense, we need to make sure the correspondence between the operator sum representation and the Bloch representation is well-defined and preserves convex sums and composition. We state the following to be complete, but the proof is routine so it is omitted.

Lemma 2.7

(1) *The identification between the operator sum representation and the Bloch representation is well-defined.*

(2) *The Bloch representation of the convex sum of quantum channels is the convex sum of the individual Bloch representations.*

(3) *The Bloch matrix of a composition of unital channels corresponds to the multiplication of the Bloch matrices.*

3 A Characterization of The Unital Diagonal Channels

The set of Bloch matrices that corresponds to the completely positive maps for $n = 1$ is the convex closure of SO(3). Unfortunately for $n \geq 2$, $\mathcal{U}_n$ is not a well-known set. The set of Bloch diagonal matrices on one qubit is well-studied and a characterization of the Bloch diagonal channels on n-qubits was given in [1] but not rigorously proven for any finite dimensional system. We will give a proof, but first we need a little structure to prove the theorem.

One can compute $\sigma_j \sigma_i \sigma_j = \pm\sigma_i$. Given that for $m \times m$ matrices r, s, t, and u, $(r \otimes s)(t \otimes u) = (rt \otimes su)$, we have $\lambda_j \lambda_i \lambda_j = \pm\frac{1}{2^{n-1}}\lambda_i$. To characterize the diagonal unital channels, we need an efficient way of keep track of the signs.

Lemma 3.1 *The sign of $\lambda_j^n \lambda_i^n \lambda_j^n$ is determined by $H_{ij}^{\otimes n}$, the (i,j) entry of the n-fold tensor product of*

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

Proof. In one dimension, if i or j is 1 or if $i = j$, then $\sigma_j \sigma_i \sigma_j = \sigma_i$. Since the Pauli matrices anti-commute, if $i \neq j$ and $i, j \neq 1$, $\sigma_j \sigma_i \sigma_j = -\sigma_j \sigma_j \sigma_i = -\sigma_i$. Thus, the assertion is true for the one-dimensional spin operators

Now suppose for $i, j \leq 2^{2k}$, that $\lambda_j^k \lambda_i^k \lambda_j^k = \frac{1}{2^{k-1}} H_{ij}^{\otimes k} \lambda_i^k$. By construction, for any two of the $(k+1)$-dimensional spin operators, λ_i and λ_j (note we dropped the $k+1$ for ascetics), there exists $i', j' \leq 2^{2k}$ and $i_1, j_1 \in \{1, 2, 3, 4\}$ so that

$$\lambda_i = \frac{1}{\sqrt{2}} \sigma_{i_1} \otimes \lambda_{i'}^k \text{ and } \lambda_j = \frac{1}{\sqrt{2}} \sigma_{j_1} \otimes \lambda_{j'}^k.$$

By induction, $\lambda_{j'}^k \lambda_{i'}^k \lambda_{j'}^k = \frac{1}{2^{k-1}} H_{i'j'}^{\otimes k} \lambda_{i'}^k$, and so

$$\lambda_j \lambda_i \lambda_j = \frac{1}{2^k} (\sigma_{j_1} \sigma_{i_1} \sigma_{j_1}) \otimes (\lambda_{j'}^k \lambda_{i'}^k \lambda_{j'}^k) = \frac{1}{2^k} H_{i_1 j_1} H_{i'j'}^{\otimes k} \sigma_{i_1} \otimes \lambda_{i'}^k = \frac{1}{2^k} H_{ij}^{\otimes k+1} \lambda_i.$$

□

Now suppose $\{A_j\}_{j=1}^k$ is a set of linearly independent matrices, and let $\Phi : H_{2^n} \to H_{2^n}$ be defined by $\Phi(\rho) = \sum_i \beta_i A_i \rho A_i^\dagger$. By a result in [1], Φ is completely positive if and only if $\beta_i \geq 0$ for every i; we will use this result in the following. Please note that the next theorem was stated by Bourdon and Williams in [1], but they only gave a sketch of the proof. We claim no originality to the statement of the theorem, but since this result will be used throughout this note, we give a full proof and correct some discrepancies.

Theorem 3.2 *Let $N = 2^n$, $r \in \mathbb{R}^{2^{2n}-1}$ and $\Phi_D : H_N \to H_N$ be defined by*

$$\Phi_D(r_1 I + r \cdot \lambda) = r_1 I + (Dr) \cdot \lambda$$

where

$$D = \begin{pmatrix} d_2 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & d_N \end{pmatrix} \text{ and let } d' = \begin{pmatrix} 1 \\ d_2 \\ \vdots \\ d_N \end{pmatrix}.$$

Then $D \in U_n$ if and only if $H^{\otimes n} d'$ has all non-negative entries.

Proof. This operator is by definition linear and trace preserving regardless of D; also, $\Phi_D(I) = I$. Next we can calculate the action of Φ_D on λ_j for each $j \geq 2$:

$$\Phi_D(\lambda_j) = \Phi_D(e_j \cdot \lambda) = (De_j) \cdot \lambda = d_j \lambda_j,$$

where e_j is the j^{th} coordinate vector. So we have characterized Φ_D by its action on the basis of n-dimensional spin operators.

Consider the linear operator $\Phi : H_{2^n} \to H_{2^n}$ defined by $\Phi(\rho) = \sum_i \beta_i \lambda_i \rho \lambda_i$, where each $\beta_i \in \mathbb{R}$. From Lemma 3.1, $\Phi(\lambda_j) = \frac{1}{2^{n-1}}(\sum_i H_{ij}^{\otimes n} \beta_i)\lambda_j$. Let $\beta = 2^{n-1} H^{\otimes n} d'$, then $d_i = \frac{1}{2^{n-1}} \sum_j H_{ij}^{\otimes n} \beta_j$ and $\frac{1}{2^{n-1}} \sum_i \beta_i = 1$. This choice of β_i gives $\Phi(\lambda_j) = \Phi_D(\lambda_j)$ for every j and since linear operators are completely determined by their action on a basis, this implies $\Phi_D = \Phi$. From the earlier discussion on complete positivity and given the fact that the n-dimensional spin operators are linearly independent, Φ_D is completely positive if and only if each $\beta_i \geq 0$. This is equivalent to $\frac{1}{2^{n-1}} \beta = H^{\otimes n} d'$ having all non-negative entries. □

For the duration we will refer to d' as the vector associated to the diagonal channel D.

4 The Free Affine Monoid Over The Involution Groups

Definition 4.1 An *involution group* is a set with a binary operation, $(S, \cdot)$, and an identity element 1, where $(\forall x \in S)\ x \cdot x = 1$.

By the classification of finite abelian groups and some basic algebra, S is a finite involution group if and only if it is isomorphic to the direct product of Z_2 k-times, $\mathbb{Z}_2^k$.

The involution group in $(2, 2)$ of order 2 is

$$V_2 = \left\{ I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, f = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}.$$

From [9] (and also unknowingly in [3]) we can recursively generate Z_2^n in the $(2^n, 2^n)$ channels. Given $V_{2^n} = \{P_i : i = 1, \ldots, 2^n\}$ in $(2^n, 2^n)$, we construct

$$V_{2^{n+1}} = \{I_2 \otimes P, f \otimes P : P \in V_{2^n}\} \in (2^{n+1}, 2^{n+1}).$$

Note that $V_{2^{2n}} = \{I_2 \otimes I_2 \otimes P, I_2 \otimes f \otimes P, f \otimes I_2 \otimes P, f \otimes f \otimes P : P \in V_{2^{2n-2}}\}$. Given this structure, an easy induction argument (which is omitted) shows that for every $v \in V_{2^{2n}}$, there are $v_1, \ldots, v_n \in V_4$ such that $v = v_1 \otimes \cdots \otimes v_n$.

We can also recursively construct an involution group of order 2^{2n} as a subset

of $\mathcal{U}_n$. First we have

$$D_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, D_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, D_3 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, D_4 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

The set $\{D_1, D_2, D_3, D_4\} \subset \mathrm{SO}(3)$ is a copy of the Klein V group in $\mathcal{U}_1$. We can obtain D_i by placing the entires of the i^{th} row of H, starting with the second column, on the diagonal of D_i, i.e.

$$D_i = \begin{pmatrix} H_{i2} & 0 & 0 \\ 0 & H_{i3} & 0 \\ 0 & 0 & H_{i4} \end{pmatrix}.$$

We can systematically define a set of involutions in $\mathrm{SO}(2^{2n}-1)$ in a similar way; although it may not be immediately clear these involutions will be elements of $\mathcal{U}_n$ as well.

Definition 4.2 Define $G_n = \{D_i^n\}_{i=1}^{2^{2n}}$ to be the *natural representation* of the involution group of order 2^{2n} in $\mathrm{SO}(2^{2n}-1)$, where

$$D_i^n = \begin{pmatrix} H_{i2}^{\otimes n} & 0 & 0 & 0 \\ 0 & H_{i3}^{\otimes n} & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & H_{i2^{2n}}^{\otimes n} \end{pmatrix};$$

note the the exponent is for bookkeeping, not for raising D_i the n^{th} power.

Recall that for two matrices A and B, the direct sum of A and B is

$$A \oplus B = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}.$$

From the properties of the tensor product and the construction of D_i^n, for each row of $H^{\otimes n}$ there are indices $i_1, \ldots, i_n \in \{1, 2, 3, 4\}$ such that the row is equal to the diagonal of $(1 \oplus D_{i_1}^1) \otimes \cdots \otimes (1 \oplus D_{i_n}^1)$. Therefore, each D_i^n can written in terms of an n-fold tensor product of elements from the set $\{1 \oplus D_j^1\}_{j=1}^4$. Thus each D_i^n has determinant one. Also, since all the entries of D_i^n are ± 1, D_i^n is an involution, so $D_i^n \in \mathrm{SO}(2^{2n}-1)$. We will show in the following that $\langle G_n \rangle$ is convex-linearly isomorphic to $\langle V_{2^{2n}} \rangle$ and that the convex closure of G_n is equal to the set of diagonal matrices in $\mathcal{U}_n$.

Definition 4.3 Let G be a subgroup of (m, n). An *embedding* of the convex closure of G, $\langle G\rangle$, into $\mathcal{Q}_l$ is a function $\varphi : \langle G\rangle \to \mathcal{Q}_l$ such that for all $x, y \in \langle G\rangle$,

- $\varphi(I) = I$,
- $\varphi(xy) = \varphi(x)\varphi(y)$,
- $\varphi(px + (1-p)y) = p\varphi(x) + (1-p)\varphi(y)$ whenever $p \in [0, 1]$, and
- $\varphi(x) = \varphi(y) \Rightarrow x = y$.

That is, an *embedding* is an injective, convex-linear homomorphism. The set of channels $\varphi(\langle G\rangle)$ is then said to have a *classical representation.*

In [9], Martin constructs an embedding of the Klein V in $(4, 4)$ into $\mathcal{Q}_1$. It is shown in [4] that there are no other involution groups embeddable into the set of qubit channels. The question naturally arose, are there other involution groups in the higher-dimensional quantum channels that have classical representations? We will show that the answer is yes for every finite involution group!

Lemma 4.4 *Let $h^{\otimes n}$ be the n-fold tensor product of the Hadmard matrix,*

$$h = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Then $h^{\otimes 2n}$ diagonalizes $V_{2^{2n}}$ to $1 \oplus G_n = \{1 \oplus D_i^n : D_i^n \in G_n\}$.

Proof. From [5], we know that $h \otimes h$ diagonalizes V_2 to $1 \oplus G_1$. Let $v \in V_{2^{2n}}$ and $v_1, \ldots, v_n \in V_4$ such that $v = v_1 \otimes \cdots \otimes v_n$. Let $1 \oplus D_{i_j} = h^{\otimes 2} v_j h^{\otimes 2}$. Then $h^{\otimes 2n} v h^{\otimes 2n} = h^{\otimes 2} v_1 h^{\otimes 2} \otimes \cdots \otimes h^{\otimes 2} v_n h^{\otimes 2} = (1 \oplus D_{i_1}) \otimes \cdots \otimes (1 \oplus D_{i_n})$. By the discussion in the preceding paragraph, the latter is an element of $1 \oplus G_n$. □

Corollary 4.5 *The n-fold tensor product of the Hadamard matrix diagonalizes V_{2^n}.*

What we have shown is that there is an isomorphism between the affine monoids $\langle V_{2^{2n}}\rangle$ and $\langle G_n\rangle$ that is defined by conjugation. An affine monoid is a convex subset of a real algebra that contains an identity and is closed under multiplication. For example, given a group G the convex closure of G, denoted $\langle G\rangle$, is an affine monoid. In certain cases, the affine monoid $\langle G\rangle$ is called the free affine monoid over G.

Definition 4.6 A *free affine monoid* over a finite group G is an affine monoid $\langle G\rangle$ such that each homomorphism $f : G \to \mathbb{A}$ into an affine monoid $\mathbb{A}$ has a unique convex-linear extension to all of $\langle G\rangle$.

From [8], the free affine monoid over every finite group exists and is unique up to convex-linear isomorphism. More importantly, it is shown in [8] that $\langle V_{2^n}\rangle$ is the free affine monoid over the involution group of order 2^n.

Theorem 4.7 *For every $j \in \mathbb{N}$ there is an $n \in \mathbb{N}$, such that $\langle V_{2^j}\rangle$ is embeddable into $\mathcal{Q}_n$ via conjugation. That is, every finite involution group has a classical and quantum representation. Moreover, $\langle G_n\rangle \subset \mathcal{U}_n$ and $\langle G_n\rangle$ is the free affine monoid over the involution group of order 2^{2n}.*

Proof. Note for all $i < j$, the involution group of order 2^j has the involution group of order 2^i as a subgroup and the restriction of an embedding is still an embedding. So we will check the claim for involution groups of order 2^{2j}.

First we show for all $D_i^n \in G_n$, that $D_i^n \in \mathcal{U}_n$. Recall that $H * H = 4I_4$ so the rows of H are orthogonal; since $H^{\otimes n}H^{\otimes n} = (H * H)^{\otimes n}$, the rows of $H^{\otimes n}$ are orthogonal as well. Let d be the vector associated with D_i^n. Since $H^{\otimes n}$ is symmetric, d is a column vector of $H^{\otimes n}$, implying the entries of $H^{\otimes n}d$ are all zero except the i^{th} entry which is 2^{2n}. Thus, all the entries of $H^{\otimes n}d$ are non-negative, and by Theorem 3.2 D_i^n is a unital channel. By Lemma 2.7, the convex sum of unital channels is unital implying $\langle G_n \rangle \subset \mathcal{U}_n$.

Since the isomorphism between $1 \oplus G_n$ and $V_{2^{2n}}$ is defined by conjugation, it is injective, preserving multiplication, convex sums, and the identity. Note that if $\sum_i x_i = 1$ and $x_i \geq 0$ for each i, then $\sum_i x_i(1 \oplus D_i) = 1 \oplus \sum_i x_i D_i$. Define $\varphi : \langle 1 \oplus G_n \rangle \to \langle G_n \rangle$ to be $\varphi(\sum_i x_i(1 \oplus D_i)) = \sum_i x_i D_i$. This is clearly a convex-linear isomorphism and by transitivity of convex-linear isomorphisms, $\langle V_{2^{2n}} \rangle$ is convex-linearly isomorphic to $\langle G_n \rangle$. Thus, $\langle V_{2^{2n}} \rangle$ is a classical representation of $\langle G_n \rangle$. By the uniqueness of free objects, $\langle G_n \rangle$ is the free affine monoid over the involution group of order 2^{2n}. □

Without embedding $V_{2^{2n}}$ into $\mathcal{U}_n$, one can show directly that $\langle G_n \rangle$ is the free affine monoid over the involution group of order 2^{2n}. By the uniqueness of the free affine monoid there must be a convex-linear isomorphism between $V_{2^{2n}}$ and G_n, however there is no reason for the isomorphism to preserve eigenvalues. Since this isomorphism is defined by conjugation, it preserves eigenvalues and therefore will preserve information theoretic quantities. Since these information theoretic quantities are preserved, there is a possibility of doing quantum information theory with classical channels under this isomorphism.

We have now laid all the necessary foundation for the second characterization of the diagonal unital channels. It was shown in [11] that the set of diagonal qubit channels is the convex closure of G_1; we have a natural extension for the set of n-qubit channels.

Theorem 4.8 *The set of diagonal channels on n-qubits is* $\langle G_n \rangle$.

Proof. First assume $D \in \mathcal{U}_n$ and D is diagonal. Let $d = [1\ d_2 \cdots d_{2^{2n}}]^t$ be the vector associated with D. Let β be the vector so that $d = H^{\otimes n}\beta$. Since the columns of $H^{\otimes n}$ define the diagonals of each $D_i \in G_n$, $d_i = \sum_j H_{ij}^{\otimes n}\beta_j = \sum_j \beta_j (D_j)_{ii}$. Therefore

$$D = \sum_{i=1}^{2^{2n}} \beta_i D_i.$$

Because we assumed that D was Bloch diagonal, Theorem 3.2 states that the entries of β are non-negative. Since the first entry of d is 1 and the first row of $H^{\otimes n}$ is all 1's, $1 = \sum_i \beta_i$; thus $D \in \langle G_n \rangle$. Conversely, $\langle G_n \rangle$ is contained in the set of diagonal unital channels by Theorem 4.7. □

With Theorem 4.7 we can see that every involution group with order less than 2^n has a classical representation in $\mathcal{U}_n$. It should be clear that $\langle G_n \rangle$ does not contain any other involutions because any element in $\langle G_n \rangle \backslash G_n$ will have an entry on the diagonal that is not ± 1. This implies that the largest involution group in $\mathcal{U}_n$ with a diagonal representation has order 2^{2n}. More importantly, $\langle G_n \rangle$ provides a legitimate higher dimensional analog to the set of diagonal qubit channels. The set is not contrived, there is a clear conceptual connection between the set of n-qubit diagonal channels and $\langle G_1 \rangle$. This provides more evidence that the work done on the set of unital qubit channels will be extendable to $\mathcal{U}_n$.

5 Arbitrary Unital Channels

As far as we know, there is no characterization of the Bloch matrices on n-qubits. This section will give conditions to disqualify an arbitrary $(2^{2n}-1) \times (2^{2n}-1)$ matrix from being unital.

Lemma 5.1 *Let $f \in \mathcal{U}_n$. Then the diagonal of f also defines a unital channel.*

Proof. Recall from Lemma 2.7 that $\mathcal{U}_n$ is closed under products and convex sums. Let $f \in \mathcal{U}_n$; we will show through a series of operations on f involving only convex sums and products of untial channels, f can be reduced to its diagonal. Let $D_k \in G_n$ and recall that $(D_k)_{ij} = 0$ if $i \neq j$ and $(D_k)_{ii} = \pm 1$. Thus,

$$(D_k f D_k)_{ij} = \sum_{r=1}^{2^{2n}-1} (D_k f)_{i,r}(D_k)_{r,j} = \pm (D_k f)_{ij} = \pm \sum_{l=1}^{2^{2n}-1} (D_k)_{i,l} f_{l,j} = \pm f_{ij},$$

where the sign of $(D_k f D_k)_{ij}$ is positive if $(D_k)_{ii} = (D_k)_{jj}$, and the sign is negative otherwise. So the diagonal of f and $D_k f D_k$ are the same, and thus $(\frac{1}{2}f + \frac{1}{2}D_k f D_k)_{ii} = f_{ii}$ for each $i \in \{1, \ldots, 2^{2n}-1\}$. Also, for every pair (i,j) where $(D_k)_{ii} \neq (D_k)_{jj}$, $(\frac{1}{2}f + \frac{1}{2}D_k f D_k)_{ij} = 0$; otherwise, $(\frac{1}{2}f + \frac{1}{2}D_k f D_k)_{ij} = f_{ij}$. Also note that $1/2(f + D_k f D_k) \in \mathcal{U}_n$ by the above remark. So if for every $i \neq j$, there was a $D_k \in G_n$ such that $(D_k)_{ii} \neq (D_k)_{jj}$, then $\sum_{k=1}^{2^{2n}} \frac{1}{2^{2n}} D_k f D_k \in U_n$, and it would have the same diagonal as f with 0 in every other entry.

To finish the proof, we need to show that for every pair (i,j), $1 \leq i < j \leq 2^{2n}-1$, there is a $D_k \in G_n$ such that $(D_k)_{ii} \neq (D_k)_{jj}$. We will show something slightly stronger: for $i \neq j$, there is a k such that $H_{ki}^{\otimes n} \neq H_{kj}^{\otimes n}$. This can be checked true for $n = 1$, and to break stride with the rest of the paper, we induct on n.

Assume that for each i and j, $1 \leq i < j \leq 2^{2n}$, there is a k such that $H_{ki}^{\otimes n} \neq H_{kj}^{\otimes n}$. Recall

$$H^{\otimes(n+1)} = \begin{pmatrix} H^{\otimes n} & H^{\otimes n} & H^{\otimes n} & H^{\otimes n} \\ H^{\otimes n} & H^{\otimes n} & -H^{\otimes n} & -H^{\otimes n} \\ H^{\otimes n} & -H^{\otimes n} & H^{\otimes n} & -H^{\otimes n} \\ H^{\otimes n} & -H^{\otimes n} & -H^{\otimes n} & H^{\otimes n} \end{pmatrix}.$$

Let $1 \leq i < j \leq 2^{2n+2}$; define $i' = i \pmod{2^{2n}}$ and $j' = j \pmod{2^{2n}}$. Note that by construction of $H^{\otimes(n+1)}$ for $2 \leq k \leq 2^{2n}$, $H_{ki'}^{\otimes n} = H_{ki}^{\otimes(n+1)}$ (similarly with j and j'). If $i' \neq j'$, then by induction there is a k, $2 \leq k \leq 2^{2n}$, such that $H_{ki'}^{\otimes n} \neq H_{kj'}^{\otimes n}$; this implies $H_{ki}^{\otimes(n+1)} \neq H_{kj}^{\otimes(n+1)}$. If $i' = j'$, then $j = r2^{2n} + i'$, where $r \in \{1, 2, 3\}$. The next arguments should be clear by the construction of $H^{\otimes(n+1)}$. If $1 \leq i \leq 2^{2n}$ and r is either 2 or 3, then for every k, $2^{2n} < k \leq 2^{2n+1}$, $H_{ki}^{\otimes(n+1)} \neq H_{kj}^{\otimes(n+1)}$. Similarly, if $r = 1$, the same is true for each k, $2^{2n+1} < k \leq 3 * 2^{2n}$. If $2^{2n} < i \leq 2^{2n+1}$, then r is either 2 or 3. In either case, for each k, $2^{2n} < k \leq 2^{2n+1}$, $H_{ki}^{\otimes(n+1)} \neq H_{kj}^{\otimes(n+1)}$. If $2^{2n+1} < i \leq 3 * 2^{2n}$, then $r = 4$ and for each k, $2^{2n+1} < k \leq 3 * 2^{2n}$, $H_{ki}^{\otimes(n+1)} \neq H_{kj}^{\otimes(n+1)}$. □

Interestingly enough, the proof of the last theorem, along with work done by Keye Martin on retractive groups, gives a bound on the scope of a unital channel: the scope of any unital channel is bounded from below by the capacity of its diagonal [10]. Moreover, Theorems 5.1 and 3.2 allow us to extend the trace lemma from [11] in a very intuitive way. We can bound the trace of an arbitrary unital channel with the following lemma.

Lemma 5.2 (The trace lemma for n-qubits) *If $f \in \mathcal{U}_n$, then $tr(f) \in [-1, 2^{2n} - 1]$, and the bounds are achieved.*

Proof. By Lemma 5.1, we only need to consider diagonal channels. For the lower bound, let D be diagonal in $\mathcal{U}_n$ with the associated vector d. By Theorem 3.2, $(H^{\otimes n}d)_1 = 1 + \mathrm{tr}(D) \geq 0$, which implies that $\mathrm{tr}(D) \geq -1$. To see the bound is achieved, observe that $\sum_i H_{2i} = 0$ and assume for $l \leq k$, $\sum_i H_{2i}^{\otimes l} = 0$. By the construction of $H^{\otimes(k+1)}$, $\sum_i H_{2i}^{\otimes k+1} = 4\sum_i H_{2i}^{\otimes k} = 0$. Since $\mathrm{tr}(D_2^{k+1}) + 1 = \sum_i H_{2i}^{\otimes(k+1)}$, we have $\mathrm{tr}(D_2^{k+1}) = -1$.

For the upper bound, let $D \in \mathcal{U}_1$ and d be the associated vector. Then

$$Hd = \begin{pmatrix} 1 + d_2 + d_3 + d_4 \\ 1 + d_2 - d_3 - d_3 \\ 1 - d_2 + d_3 - d_4 \\ 1 - d_2 - d_3 + d_4 \end{pmatrix}$$

must have non-negative entries. Summing the last three entries of Hd gives $3 - d_2 - d_3 - d_4 \geq 0$, implying that $\mathrm{tr}(D) \leq 3$. Note the sum over all the entries of Hd equals 4, canceling the d_i's. So assume for all $k \leq n$ that summing over the entries of $H^{\otimes k}d$ is 2^{2k} when d is a vector of the from $d = [1\ a_2 \cdots a_{2^{2k}}]^t$. Next let $D' \in \mathcal{U}_{n+1}$ be diagonal with $d' = [1\ d_2 \ldots, d_{2^{2(n+1)}}]^t$ as the associated vector. Let $x_1 = [1\ d_2 \ldots d_{2^{2n}}]^t$, $x_2 = [d_{2^{2n}+1}\ \ldots d_{2^{2n+1}}]^t$, $x_3 = [d_{2^{2n+1}+1}\ \ldots d_{3*2^{2n}}]^t$ and $x_4 = [d_{3*2^{2n}+1}\ \ldots d_{2^{2n+2}}]^t$. Then summing all the entries of column vector re-

sulting from

$$\begin{pmatrix} H^{\otimes n} & H^{\otimes n} & H^{\otimes n} & H^{\otimes n} \\ H^{\otimes n} & H^{\otimes n} & -H^{\otimes n} & -H^{\otimes n} \\ H^{\otimes n} & -H^{\otimes n} & H^{\otimes n} & -H^{\otimes n} \\ H^{\otimes n} & -H^{\otimes n} & -H^{\otimes n} & H^{\otimes n} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

gives $4\sum_i (H^{\otimes n}x_1)_i$, which is $4{*}2^{2n-2} = 2^{2n+2}$ by induction. Using the fact that the first entry of $H^{\otimes(n+1)}d'$ is $1 + \mathrm{tr}(D')$ and that all the entries must be non-negative, summing all but the first row will give $2^{2(n+1)} - 1 \geq \mathrm{tr}(D')$. To see that the bound is achieved, use $D_1^n = I_{2^{2n}-1}$ □

In [11], Martin proves the following proposition for $n = 1$ using the trace lemma:

Proposition 5.3

(1) *If $f \in \mathcal{U}_n$ and $f^{-1} \in U_n$, then $-f \notin \mathcal{U}_n$.*

(2) *If $f \in \mathcal{U}_n$ and orthogonal, then $f \in SO(2^{2n} - 1)$.*

(3) *If $f \in \mathcal{U}_n$, $f^{-1} \in \mathcal{U}_n$ if and only if $f \in SO(2^{2n} - 1)$.*

The proof for $n \geq 1$ is an immediate generalization of the proof given of Proposition 3.9 in [11], so we will omit it.

6 Some Remarks About the Results

We have characterized diagonal unital channels in two ways: the first is directly from the complete positivity conditions and the second as the convex hull of the unital diagonal involutions. With the second characterization, we were able to show that the diagonal untial channels form a copy of the free affine monoid over an involution group. This shows that in every dimension there are new non-trivial classes of quantum channels with a classical representation. More importantly, by Theorem 4.7, each classical channel in $\langle V_{2^{2n}} \rangle$ uniquely represents an n-qubit channel, up to change of basis. As shown in [11], we can use this fact to measure the transmission rate of classical information through any unital qubit channel from the set of diagonal unital channels and their classical representations. Although a higher-dimensional analog to calculating scope is not well studied, we hope there are information theoretic properties that can be characterized via the classical representations of quantum channels.

Moreover, in higher dimensions we are able to answer some basic questions about unital channels. For example, the antipodal map on the Bloch vector, $fx = -x$, does not define a unital channel; for the proof we just invoke the trace lemma. The trace lemma also gives a way to show that any invertible unital channel must be an orientation-preserving rotation. This is well-known, but we were able to invoke the trace lemma to prove it. More importantly, the trace lemma gives an easy-to-calculate condition that every Bloch matrix must satisfy.

It is hard to overstate the importance of the diagonal qubit channels. As shown in [7], set of teleportation channels for a single qubit is exactly the set of diagonal channels; we believe that the diagonal channels will play a large roll in the general teleportation schemes. Also, the scope of every qubit channel can be calculated using the set of diagonal channels [11]. Although we can can only bound the scope from below by the set of diagonal channels, we hope that a similar result will be true for n-qubits.

7 Acknowledgements

We would like to thank Johnny Feng for entertaining more questions than any one person should and for his helpful discussions on the formalisms of quantum channels and density matrices...we are sure at those times he wished he had a secluded office. We would also like to thank Keye Martin for many valuable discussions on quantum mechanics and for persuading us to look into this topic.

"There is something romantic about a thing that undoes itself." – K. Martin

References

[1] Bourdon, P.S, and H.T. Williams, *Unital quantum operations on the Bloch ball and Bloch region*, Phys. Rev. A. **69** (2004), 022314.

[2] Choi, M., *Completely Positive Linear Maps on Complex matrices*, Linear Algebra and Its Applications **10** (1975) 285–290.

[3] Crowder, T., and C.K. Li. *Studying Genetic Code By a Matrix Approach*. Bull of Math Bio **72** (2010) 953–972.

[4] Crowder, T., and K. Matrin. *Classical Representations of Qubit Channels*. Electronic Notes in Theoretical Computer Science **270** (2011), 37–58.

[5] Crowder, T. and K. Martin *Information theoretic representations of qubit channels*. Proceedings of Quantum Physics and Logic 2010, in press.

[6] Kimura, G., *The Bloch vector for N-level systems*. Phys Lett. A **14** (2005), 339–349.

[7] Lanzagorta, M. and K. Martin. *Teleportation with an imperfect state*. Theoretical Computer Science, Elsevier Science, submitted

[8] Martin, K., J. Feng, and S. Krishnan. *A Free Object in Quantum Information Theory*. Electronic Notes in Theoretical Computer Science **267** (2010), 35–47.

[9] Martin, K., *How to randomly flip a quantum bit*, Electronic Notes in Theoretical Computer Science **270** (2011) 81–97.

[10] Martin, K., *Retractive Groups*, Private Correspondence.

[11] Martin, K., *The scope of a quantum channel*, Submitted to Proceedings of the Clifford Lectures, American Mathematical Society.

[12] Nielsen, M., and I. Chuang, "Quantum computation and quantum information," Cambridge University Press, Cambridge (2000).

[13] Serre, D., *Matrices: Theory and applications*. Springer-Verlag, Graduate Texts in Mathematics, 2000.